IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MASSACHUSETTS

ALLIANCE FOR AUTOMOTIVE INNOVATION, Plaintiff, v. MAURA HEALEY, Attorney General of the Commonwealth of Massachusetts, in her official capacity, Defendant.	:	Case No. 1:20-cv-12090-DPW

STATEMENT OF INTEREST OF THE UNITED STATES

TABLE OF CONTENTS

INTRODUCTION

The Commonwealth of Massachusetts recently enacted a law—Massachusetts SD645, presently codified at Chapter 93K of the Massachusetts General Laws (the Data Law)—that requires motor vehicle manufacturers to provide vehicle owners and certain third parties with wireless access to particular vehicle systems. Plaintiff, the Alliance for Automotive Innovation, has brought this suit against the Attorney General of Massachusetts alleging that the Data Law is unenforceable because it is inconsistent with the National Traffic and Motor Vehicle Safety Act, 49 U.S.C. § 30101 *et seq*. (Safety Act). The United States Department of Transportation (DOT) and the National Highway Traffic Safety Administration (NHTSA), an operating administration of DOT, have broad authority to enforce the Safety Act. Pursuant to 28 U.S.C. § 517,[1] the United States of America submits this Statement of Interest to inform the Court that if in practice the Data Law's requirement of remote access to vehicles' telematics systems creates a safety issue constituting a defect under the Safety Act, then that Act would require motor vehicle manufacturers to recall and stop selling new vehicles compliant with that requirement. Although this action also includes a claim that the Safety Act preempts the Data Law, the United States takes no position on that claim at this time.[2]

[1] Section 517 provides that the "Solicitor General, or any officer of the Department of Justice, may be sent by the Attorney General to any State or district in the United States to attend to the interests of the United States in a suit pending in a court of the United States, or in a court of a State, or to attend to any other interest of the United States." 28 U.S.C. § 517.

[2] Because the Data Law was enacted so recently, no motor vehicle manufacturers have actually made any complying modifications to their vehicles. Moreover, the rapidly changing nature of cybersecurity safety only increases the difficulty for DOT in making a fact-intensive determination as to whether any potential changes made by motor vehicle manufacturers to comply with the Data Law would result in a defect related to motor vehicle safety.

STATUTORY BACKGROUND

The Safety Act's purpose is "to reduce traffic accidents and deaths and injuries resulting from traffic accidents." 49 U.S.C. § 30101. Foundational to the Safety Act is "motor vehicle safety," which is defined as "the performance of a motor vehicle or motor vehicle equipment in a way that protects the public against unreasonable risk of accidents occurring because of the design, construction, or performance of a motor vehicle, and against unreasonable risk of death or injury in an accident, and includes nonoperational safety of a motor vehicle." *Id*. § 30102(a)(9).

The Safety Act requires the Secretary of Transportation to "prescribe motor vehicle safety standards." *Id*. § 30111(a) (vehicle standards).[3] Motor vehicle manufacturers must certify that vehicles comply with these standards. *Id*. § 30115. The Act also requires motor vehicle manufacturers to recall a vehicle if they determine that the vehicle contains a defect in performance, construction, a component, or a material "related to motor vehicle safety." *See, e.g.*, *id*. § 30116; *see also id*. §§ 30111, 30118.[4] A recall involves reporting the defect to DOT, notifying affected owners, and providing owners with a free repair, refund, or replacement vehicle. *See id.* §§ 30118-20. A motor vehicle manufacturer is prohibited from selling (or offering for sale) new motor vehicles that are subject to a recall. *Id*. § 30112(a).

DOT has broad authority to enforce the Safety Act. This authority includes the ability to conduct investigations into whether a defect or compliance failure exists, to order recalls if necessary, to ensure the adequacy of recalls, and to pursue civil penalties for violations of the law. *See id*. §§ 30165-66, 30118-20. Although DOT is authorized to issue recall orders, in practice, the

[3] DOT has delegated the authority to enforce the Safety Act to NHTSA. 49 C.F.R. § 1.95(a).

[4] A recall is required based solely on the existence of a safety-related defect, even if no vehicle standard otherwise applies to the defective vehicle component or issue.

agency typically works with a motor vehicle manufacturer to comply with that manufacturer's affirmative legal obligation to self-initiate a recall, rather than face the prospect of a recall order.[5]

FACTUAL AND PROCEDURAL BACKGROUND

In 2020, voters in Massachusetts approved a ballot initiative enacting the Data Law. *See* Compl. ¶ 1, ECF No. 1. Generally, the law requires motor vehicle manufacturers to provide vehicle owners and non-dealership vehicle repair facilities (repair facilities) with wireless access to their vehicles' telematics systems.[6] Vehicle telematics systems are defined as "any system in a motor vehicle that collects information generated by the operation of the vehicle and transmits such information . . . utilizing wireless communications to a remote receiving point where it is stored." Mass. Gen. Laws Ann. ch. 93K, § 1.

Specifically, the Data Law requires motor vehicle manufacturers to equip all vehicles using telematics systems for model years 2022 and afterward "with an inter-operable, standardized and open access platform across all makes and models that is capable of securely communicating all

[5] *See United States v. Gen. Motors Corp.*, 574 F. Supp. 1047, 1049 (D.D.C. 1983) (explaining that the Safety Act "imposes an independent duty upon manufacturers of motor vehicles to give notification of and to remedy known safety-related defects" and that "[t]he duty exists with or without a Secretary's order to that effect"); NHTSA, *Risk-Based Processes for Safety Defect Analysis & Management of Recalls* at 10 (Nov. 2020), https://www.nhtsa.gov/sites/nhtsa.gov/files/documents/14895_odi_defectsrecallspubdoc_110520-v6a-tag.pdf ("If necessary, NHTSA also has the statutory authority to make a formal decision that a vehicle or equipment contains a safety-related defect and can order a manufacturer to conduct a recall."); *id.* at 12 ("A recall is typically initiated when a manufacturer files a Part 573 Defect Information Report identifying a safety defect, often called a DIR or Part 573 Report.").

[6] The United States recognizes that interoperability and compatibility requirements can promote competition and expand consumer choice. *See generally* Fed. Trade Comm'n, *Nixing the Fix: An FTC Report to Congress on Repair Restrictions* (May 2021), https://www.ftc.gov/system/files/documents/reports/nixing-fix-ftc-report-congress-repair-restrictions/nixing_the_fix_report_final_5521_630pm-508_002.pdf. However, as described below, the Data Law's specific remote access requirements, as written and currently implemented, raise potentially serious safety issues as well.

telematics vehicle data in a standardized format via direct data connection to the platform." *Id*. § 3. This platform must be "directly accessible by the [vehicle's] owner . . . through a mobile-based application" and upon the owner's authorization, by repair facilities. *Id*. Importantly, such access must include "the ability to send commands to in-vehicle components if needed for purposes of maintenance, diagnostics, and repair." *Id*. The Data Law became effective December 3, 2020. *See* Mass. Const. Amends. Art. 48, Pt. V, § 1.

In November 2020, Alliance for Automotive Innovation, an advocacy group for the motor vehicle industry, filed the present action against the Attorney General of Massachusetts. The group alleges that the Data Law is unenforceable because it is preempted by the Safety Act and other federal laws.[7] *See* Compl. ¶¶ 94-159. Specifically, Plaintiff contends that because the Data Law conflicts with, or poses an obstacle to, the purposes of the Safety Act, the Data Law is conflict preempted. *See id*. ¶¶ 94-106. Plaintiff also alleges that the Data Law constitutes an unlawful taking. *See id*. ¶¶ 160-70. Plaintiff seeks preliminary and permanent injunctive relief declaring the Data Law to be unenforceable. *See id*. ¶¶ 171-80 & Prayer for Relief.

After Plaintiff sought preliminary injunctive relief, *see* ECF No. 26, the Court consolidated the motion with adjudication on the merits, and set a bench trial for June 14, 2021. *See* Scheduling Order, ECF No. 78.

[7] Plaintiff also alleges that the Data Law is preempted by the Clean Air Act, 42 U.S.C. § 7401 *et seq*.; Copyright Act, 17 U.S.C. § 101 *et seq*.; Defend Trade Secrets Act, 18 U.S.C. § 1836 *et seq*.; Computer Fraud & Abuse Act, 18 U.S.C. § 1030; and the Digital Millennium Copyright Act, 17 U.S.C. § 1201. The United States also takes no position on Plaintiff's claims regarding these laws, nor with respect to Plaintiff's claim of an unlawful taking.

ARGUMENT

If in Practice the Data Law's Requirement of Remote Access to Motor Vehicle Telematics Systems Creates a Safety Issue Constituting a Defect Under the Safety Act, Then the Act Would Require Motor Vehicle Manufacturers to Recall and Stop Selling Vehicles Compliant With That Requirement.

The Safety Act requires motor vehicle manufacturers to recall a vehicle if they determine that it contains a defect in performance, construction, a component, or a material "related to motor vehicle safety." *See* 49 U.S.C. § 30116; *see also id*. § 30120 (establishing remedies for defects). Such manufacturers also are prohibited from selling (or offering for sale) new motor vehicles that are subject to a recall for a defect related to motor vehicle safety. *Id*. § 30112(a)(3). A "defect" is any deficiency "in performance, construction, a component, or material of a motor vehicle or motor vehicle equipment." *Id*. § 30102(a)(3).

Under the Act, a defect relates to "motor vehicle safety" if it interferes with the performance of a motor vehicle in a way that leaves the public unprotected "against unreasonable risk of accidents occurring because of the design, construction, or performance of a motor vehicle, and against unreasonable risk of death or injury in an accident." 49 U.S.C. § 30102(a)(9). *See, e.g.*, *United States v. Gen. Motors Corp*., 561 F.2d 923, 924 (D.C. Cir. 1977) (per curiam) (failure of steering pitman arms causing driver to lose control of car demonstrated unreasonable risk of accidents stemming from defect related to motor vehicle safety); *United States v. Gen. Motors Corp*., 565 F.2d 754, 757-60 (D.C. Cir.1977) (carburetor defect resulting in sudden engine fires related to motor vehicle safety); *United States v. Ford Motor Co*.,453 F. Supp. 1240, 1250 (D.D.C. 1978) (defect in windshield wiper pivot assemblies constituted defect related to motor vehicle safety due to impaired visibility).

"The purpose of the Safety Act . . . is not to protect individuals from the risks associated with defective vehicles only after serious injuries have already occurred; it is to prevent serious

injuries stemming from established defects before they occur." *Gen. Motors Corp.*, 565 F.2d at 759. Thus, in 2015, Fiat Chrysler Automobiles (FCA) ordered a vehicle recall based on a cybersecurity issue related to unsecured remote access to vehicles that had not resulted in any injuries. *See* NHTSA Recall No. 15V-461, https://static.nhtsa.gov/odi/rcl/2015/RCLRPT-15V461-9313.pdf; NHTSA Recall No. 15V-508, https://static.nhtsa.gov/odi/rcl/2015/RCLRPT-15V508-4239.pdf; *see also* Aaron M. Kessler, *Fiat Chrysler Issues Recall Over Hacking*, N.Y. TIMES (July 24, 2015), https://www.nytimes.com/2015/07/25/business/fiat-chrysler-recalls-1-4-million-vehicles-to-fix-hacking-issue.html. FCA learned that a cybersecurity researcher had wirelessly accessed one of its vehicles through an open wireless access point in the vehicle's infotainment system, and had gained control over the vehicle's engine, brakes, and steering system. *See id*. The manufacturer determined that the remote modification and control of the vulnerable vehicles could allow a bad actor to control safety critical systems on one or multiple vehicles at the same time remotely, leading to deaths or serious injuries. *See id*. As a result, and in accordance with its Safety Act obligations, FCA recalled over 1.4 million vehicles for software security vulnerabilities in order to close the open access. *See id*.

DOT is concerned that the Data Law potentially creates a similar serious cybersecurity risk to motor vehicle safety by effectively requiring open remote access to certain vehicle systems through the removal of existing manufacturer access controls. *See* Letter from James C. Owens, Deputy NHTSA Administrator, to Rep. Tackey Chan & Sen. Paul R. Feeney (Jul. 20, 2020) (attached as Ex. 1). Generally, the Data Law requires motor vehicle manufacturers to provide vehicle owners and repair facilities with wireless access to their vehicles' telematics systems. More specifically, it requires manufacturers to equip all vehicles using telematics systems for model years 2022 and onward with "an inter-operable, standardized and open access platform

across all of the manufacturer's makes and models." Mass. Gen. Laws Ann. ch. 93K § 3. This platform must be "directly accessible by the owner . . . of the vehicle through a mobile-based application and upon [his or her] authorization . . . all mechanical data shall be directly accessible by an independent motor vehicle repair facility" for the amount of time necessary to complete repairs. *Id*. Importantly, such open access must "include the ability to send commands to in-vehicle components if needed for purposes of maintenance, diagnostics, and repair." *Id*. Because all motor vehicle components potentially need maintenance, diagnostics, or repair at some point during their existence, this requirement effectively requires motor vehicle manufacturers to provide remote access to send commands to all of a vehicle's systems—including braking, steering, and acceleration. This complicated task is made even more difficult due to the timing constraints imposed by the Data Law. Given the requirement that these modifications be implemented in all motor vehicles using telematics systems for model years 2022 and onward, DOT is concerned about whether there is sufficient time to develop such a system safely and effectively.

The Data Law also mandates that access for motor vehicle owners and independent repair facilities to a vehicle's on-board diagnostic systems "shall be standardized" and must "not require any authorization by the manufacturer, directly or indirectly, unless that authorization system for access to vehicle networks and their on-board diagnostic systems is standardized across all makes and models sold in [Massachusetts] and is administered by an entity unaffiliated with a manufacturer." *Id*. § 2. Thus, Section 2 of the Data Law prohibits motor vehicle manufacturers from securing "vehicle networks and their on-board diagnostic systems" to ensure that only those entities permitted under the law have access to these critical systems unless there is an authorization system (1) that is standardized across all makes and models, (2) that does not rely on

manufacturer authorization, and (3) that is administered by a third party who is not affiliated with the manufacturer. *Id*.

Reading Sections 2 and 3 of the Data Law together, a motor vehicle manufacturer may not implement controls over remote access to any systems of a model year 2022 or later vehicle, unless those controls are administered by an unaffiliated third party. *See id*. §§ 2-3. However, the United States is not aware of any such third party that currently exists, or one that could likely be offered, operationalized, and scaled up to meet the Data Law's requirements in the necessary timeframe. *See* Ex. 1 at 3. Therefore, because a motor vehicle manufacturer is prohibited from taking any action on its own to ensure that access is limited to the owner or, with permission, an independent repair facility, the Data Law effectively requires open remote access, potentially accessible by anyone, to all of a motor vehicle's telematics systems. *See id*.

Based on DOT's current state of knowledge, this open-access requirement has the potential to create serious safety problems for motor vehicle owners. Specifically, the Data Law requires motor vehicle manufacturers to take actions that potentially pose serious cybersecurity risks by opening uncontrolled access to vehicle firmware that executes safety-critical functions, such as steering, acceleration, and braking, which are designed in a manner that expect (and require) authenticated privileged access rights in existing implementations. Such access could allow a hacker operating remotely to access these vehicle functions, and cause a severe crash, potentially leading to deaths or serious injuries. *See id*. at 2-3. Indeed, similarly (as noted above), open uncontrolled access as contemplated by the Data Law allowed security researchers to exploit software security vulnerabilities in certain FCA vehicles such that those researchers could manipulate the vehicles' safety-critical systems remotely. That manipulation led that manufacturer to recall over 1.4 million of its vehicles. This 2015 recall illustrates DOT's concerns about the

Data Law's requirements. Although that recall did not involve a malicious actor, the Safety Act is preventive and does not require actual harm to occur before a recall is required. *See Gen. Motors Corp.*, 565 F.2d at 759.

The open access effectively required by the Data Law thus has the potential to cause serious safety problems for motor vehicle owners and to frustrate the ability of motor vehicle manufacturers to follow their obligations to ensure vehicle safety. Among these obligations is the Safety Act's requirement that manufacturers must recall and stop selling new motor vehicles if they determine that their vehicles contain a defect in performance, construction, a component, or a material "related to motor vehicle safety." *See* 49 U.S.C. §§ 30112(a)(3), 30116, 30118. Because the open access mandated by the Data Law could create a potential vulnerability in vehicle cybersecurity, it may constitute a defect "related to motor vehicle safety." However, as noted above, *see supra* n.2, it is difficult for DOT to render such a fact-intensive determination at present because no motor vehicle manufacturers have to date modified their vehicles in response to the law, and because cybersecurity safety by nature rapidly changes.

Moreover, motor vehicle manufacturers may not be able to tailor vehicle production and distribution to fit the Massachusetts-specific requirements of the Data Law, leading to these cybersecurity risks effectively becoming widespread. And if other states were to enact different versions of this law, the result would be a variety of different state requirements, each with a unique potential cybersecurity risk affecting motor vehicle safety.

CONCLUSION

For the foregoing reasons, if in practice the Data Law's requirement of remote access to motor vehicles' telematics systems creates a safety issue constituting a defect under the Safety Act, then the Act would require motor vehicle manufacturers to recall and stop selling vehicles

compliant with that requirement. The United States takes no position at this time regarding whether the Data Law is preempted by the Safety Act.

Dated: June 11, 2021

Respectfully submitted,

MICHAEL D. GRANSTON
Deputy Assistant Attorney General

JACQUELINE COLEMAN SNEAD
Assistant Branch Director

/s/ *Daniel Riess*
DANIEL RIESS (Texas Bar # 24037359)
Trial Attorney
U.S. Department of Justice
Civil Division, Federal Programs Branch
1100 L Street, N.W.
Washington, D.C. 20005
Telephone: (202) 353-3098
Fax: (202) 616-8460
Email: Daniel.Riess@usdoj.gov
Attorneys for Defendants

CERTIFICATE OF SERVICE

I certify that on June 11, 2021, I caused a copy of the foregoing to be filed electronically and that the document is available for viewing and downloading from the ECF system. Participants in the case who are registered CM/ECF users will be served by the CM/ECF system. If any counsel of record requires a paper copy, I will cause a paper copy to be served upon them by U.S. mail.

/s/ *Daniel Riess*